REMARKS/ARGUMENTS

1.) Claim Amendments

The Applicant has amended claims 1, 8 and 19; claims 13-18 have been withdrawn. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-12 and 18-22 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Claim Rejections – 35 U.S.C. § 112

The Examiner objected to claims 8-12 and 19-22 under 35 U.S.C. § 112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Appropriate corrections have been made to independent Claims 8 and 19. The Examiner's favorable reconsideration is therefore respectfully requested.

3.) Claim Rejections – 35 U.S.C. § 103 (a)

The Examiner rejected claims 1-5 under 35 U.S.C. § 103(a) as being unpatentable over Tabuki (US 5,841,970) in view of Kippenhan (US 2002/0010769), in further view of Ishibashi (US 6,728,379), in further view of Hammond (US 2003/078927). The Applicant respectfully traverses the Examiner's rejection and has further amended the pending claims to more clearly and distinctly claim the subject matter which the Applicant considers as his invention. A favorable reconsideration in view of the above amendments and the following remarks is earnestly requested.

The Applicant submits that the present invention deals with not only authenticating a particular subscriber, but also with determining whether a particular mobile station has authority to access a particular database record maintained by a database server. In response to a determination that the mobile station indeed has the authority to access that particular database record within the database server, the authentication server than instructs the database server to provide the requested information to the mobile station. In accordance with the teachings of the present

invention, the authentication server further provides a key enabling the mobile station to decrypt the information received from the database server.

Accordingly, when the mobile station first authenticates with the authentication server, the authentication server provides the mobile station with a first key. This first key is then used by the mobile station when requesting access to a certain database record within a database server. In response to a determination that the mobile station has the authority to access the requested database record, the authentication server performs the following two steps: (1) instructs the database server to provide the requested information to the mobile station wherein the information is encrypted; and (2) provides the mobile station with a second key enabling the mobile station to decrypt the encrypted information received from the database server.

The Applicant respectfully submits that the cited references fail to anticipate or render obvious each and every element of the presently pending independent Claims. More specifically, none of the cited references discloses a "first key" being provided by the authentication server to a mobile station wherein such key is later submitted by the mobile station to a database server to request access to a particular database record. Even though the Examiner incorrectly cited Tabuki (Col. 6, lines 11-47) and Kippenhan (claim 34) as allegedly disclosing this novel step, the Applicant respectfully submits that the Tabuki invention actually requests such authentication data from the user host and does not provide a "first key" as claimed in the present application. Moreover, the cited portion of Tabuki (Col. 6, lines 11-47) is a mere description of Fig. 4 of Tabuki illustrating the data structure of Tabuki's relational database (RDB) record and has nothing to with the claimed step of providing "a first key to said mobile station in response to said authentication". In further accordance with the present invention, the first key provided by the authentication server is then submitted by the mobile station when requesting access to a particular database record within a database server. The database server then sends another authentication request with the submitted first key to the authentication server requesting whether that mobile station has the authority to access that particular database record. The Applicant submits that nothing in Tabuki or Kippenhan discloses or teaches such claimed elements.

Additionally, nothing in Tabuki discloses or teaches the step of "determining whether said mobile station has authority to access said particular database record" as currently claimed. More specifically, Tabuki merely authenticates a particular application client against an application server and fails to discuss or disclose the "authorization" process regarding a particular database record as currently claimed. In other words, not all data records stored within the database server are accessible by a particular mobile station and nothing in Tabuki discloses this selectively authorization process using the first key as claimed by the present invention.

Lastly, nothing in Tabuki or Ishibashi discloses or teaches the steps of "instructing said database server to provide information associated with said requested database record to said mobile station wherein said information is encrypted" and further "providing said mobile station within a second key enabling said mobile station to decrypt said information received from said database server using said second key." In accordance with the teachings of the present invention, the requested information is provided by the database server to the requesting mobile station while encrypted. The authentication server then separately provides the mobile station with yet another key (the second key) to enable the mobile station to decrypt the information received from the database server. Applicant respectfully submits that nothing in Tabuki or Ishibashi anticipates or rendered obvious these recited steps. As a matter of facts, other than disclosing the authentication process for a particular client, no further information disclosure or database sharing is discussed in Tabuki. As for Ishibashi, other than using "encryption" for transmitting information between a data transmitter and receiver, it simply fails to anticipate or render obvious the present invention.

The Applicant further submits that Kippenhan as well as Hammond similarly fail to anticipate or render obvious, independently or in combination with Tabuki or Ishibashi, the recited elements of the presently pending claims.

For at least the reasons as provided above, the Applicant submits that independent Claim 1 and its dependent claims are now patentable over the cited references and a Notice of Allowance is respectfully requested.
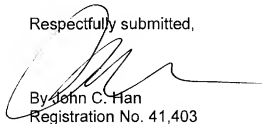
The Examiner further rejected independent Claims 8 and 19 under similar rejections (other than not applying the Kippenhan reference) as provided above for rejecting independent Claim 1. The Applicant respectfully submits that in view of the above amendments and the remarks, independent Claims 8 and 19 are likewise patentable over the cited references. A Notice of Allowance for independent Claims 8 and 19 and their respective dependent claims is respectfully requested.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

By John C. Han
Registration No. 41,403

Date: March 28, 2006

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-7686
john.han@ericsson.com